Security Automation Conference & Workshop

Sponsors

National Institute of
Standards & Technology
Defense Information Systems Agency
Department of Homeland Security
National Security Agency

Located in the Green Auditorium at the 550 acre NIST Campus in Gaithersburg, Maryland.

September 18 - 19, 2006

NIST Campus, Gaithersburg, MD USA

Learn How IT Systems Security Implementation is being automated to enable:

FISMA and other Security Compliance

Hear from Distinguished Security Speakers from Government, Industry and Academia

Richard Hale, Chief Information Assurance Officer, DISA
Dennis Heretick, Chief Information Security Officer, DOJ
Annabelle Lee, Director Security Standards, DHS
Peter Mell, National Vulnerability Database Lead, NIST
Stephen Quinn, Security Automation Project Lead, NIST
Ron Ross, FISMA Implementation Project Lead, NIST
Tony Sager, Chief, Vulnerability Analysis & Ops, NSA

Additional Information:

checklists.nist.gov

Detailed Description:

Implementing cost-effective, risk-based information security programs continues to be a top priority for federal, state, and local governments as well as private sector enterprises. Improving the security of information systems and demonstrating compliance to laws, directives, regulations, standards, and guidance can present some unique challenges to organizations. These challenges can include, for example, the selection and implementation of appropriate security controls for information systems and the associated compliance-related activities to demonstrate security control effectiveness.

This conference and workshop presents projects and integration efforts that propose to facilitate the automation of certain aspects of an organization's information security program. A key automation effort includes converting English text contained in various security-related publications (i.e., NIST Special Publication 800-53, DISA security guidance, configuration guides, checklists, etc) into machine readable formats (e.g., XML/XCCDF and OVAL). The objective of this automation effort is to provide a common understanding and semantic context for organizations and individuals using scanning tools and checklists/configuration guides and auditors conducting assessments of security control effectiveness. The end result will promote the use of commercial off-the-shelf (COTS) tools to automatically check the security properties of information systems and effectively map security compliance requirements.